www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Опыт участия в проекте «Киберустойчивый регион»

Игорь Первушин – руководитель направления
создания базы знаний компании CyberOK

В этой статье расскажем, как компания СайберОК совместно с коллегами из Innostage и Positive Technologies участвовали в проекте «Киберустойчивый регион» — на масштабе целого региона РФ.

* *Важное объявление: все данные приведенные на экранах являются тестовыми и не отображают реальное состояние защищенности какой-либо организации или групп организаций.*

Зачем всё это?

Как людям, принимающим решение на государственном уровне, понять, насколько защищён регион в целом и ключевые организации в частности? Как предоставить владельцам информационных систем статус защищенности, его изменение и те проблемы, которые им необходимо устранять в первую очередь?

В ответах на эти вопросы и заключалась цель нашего участия в проекте. При этом мы были сфокусированы на оценке поверхности атак на ресурсы, которые доступны из сети Интернет, как на области, в которой мы наиболее компетентны.

Русский Shodan

Мы в CyberOK разрабатываем СКИПА — Систему Контроля и Информирования о Поверхности Атак, которую часто называют русским Shodan-ом. Одна из наших задач – постоянный мониторинг всего пространства Рунета, но с важной оговоркой: анализ осуществляется на неполную, но достаточную глубину. Всегда приходится соблюдать тонкую грань, чтобы и пользу приносить, и не докучать лишними сетевыми пакетиками.

CyberOK и сканирования

Но в рамках проекта «Киберустойчивый регион» этого было мало, так как поставленная задача требовала гораздо более глубокого анализа, что в итоге породило множество технических и организационных моментов, которые будут рассмотрены ниже.

Главная головная боль — создать рейтинг

А сейчас хотелось бы начать с конца. Главным вызовом для нас было создать сам рейтинг (метрики и их графическое представление), потому что в нем необходимо было совместить две, как может показаться, абсолютно непересекающиеся характеристики:

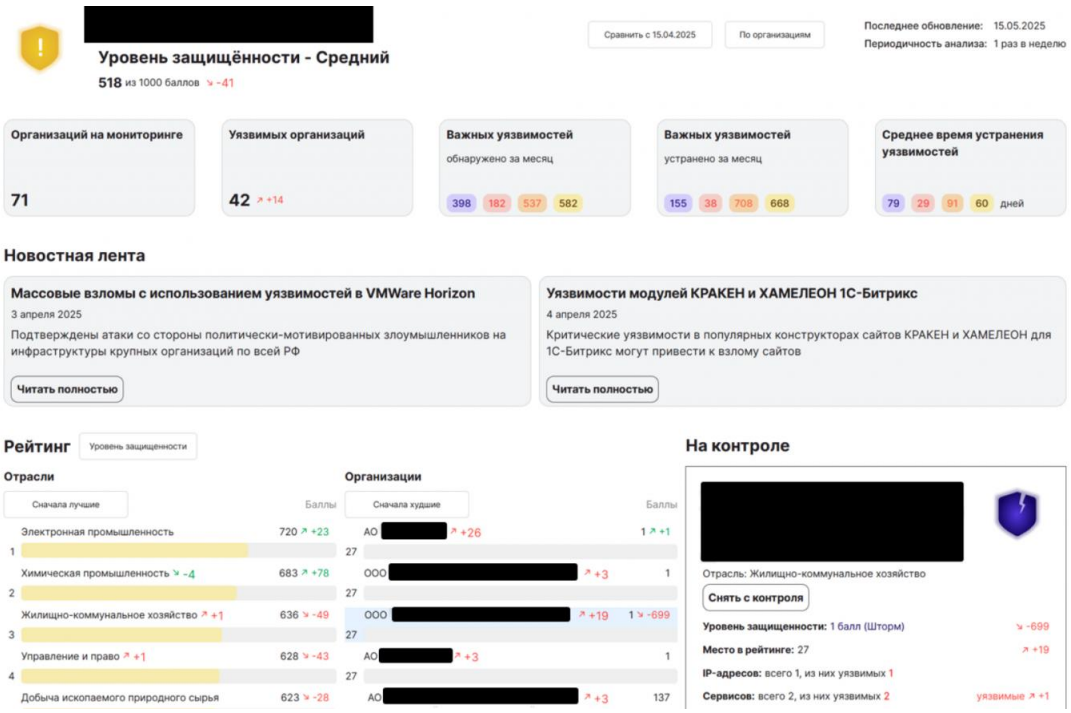
1. Понятность для широкого круга лиц. Рейтинг должен давать возможность получить текущее состояние и динамику для не всегда погруженных в IT и в конкретные проблемы с безопасностью людей;

2. Наличие прикладных данных. Рейтинг должен отражать понятную и верифицируемую информацию о том:

- Какие проблемы наиболее актуальны для той или иной организации.

- Как происходит прогресс по повышению уровня защищенности.
- На чем необходимо сконцентрироваться (организации, сферы экономики и т.д.).

Не будем погружаться в подробности расчета, пройдемся по основным элементам интерфейсам и болям, которые они решают.



Интерфейс уровня региона с детализацией на уровне организаций

Первым на очереди — дашборд уровня региона с разбивкой по организациям. Практически все метрики отвечают на 2 вопроса: на каком уровне мы находимся на текущий момент и какую динамику мы имеем?

Каждому пилоту нужна минимальная приборная панель для оценки ситуации – именно эту функцию выполняет первый блок, предоставляя основные показатели.

Внутри дашборда:

- Уровень защищенности региона (по шкале от 0 до 1000);
- Общее количество организаций под мониторингом и количество тех, у кого проблемы;
- Статистика с результатами исправления уязвимостей организациями: сколько уязвимостей найдено за месяц, сколько исправлено за месяц, среднее время реакции;
- Новостная лента с трендовыми угрозами с возможностью посмотреть, какие организации им подвержены.

Итак, первую информацию получили, что же со всем этим делать? Логичным шагом является построение рейтинга отраслей и организаций, требующих внимания. Поскольку ситуация с информационной безопасностью у участников может быть разной, была реализована возможность сортировки с выделением лидеров и отстающих. При этом, если ситуацию на уровне отраслей можно держать в голове, то с организациями это сделать очень трудно просто из-за количества, поскольку счет может идти на тысячи. Поэтому мы сделали функцию «Взятие на контроль», специально для отличившихся в худшую сторону или представляющих некий интерес организаций. Ответственный за информационную безопасность региона при помощи данного механизма может сконцентрировать свое внимание и понаблюдать за ситуацией на протяжении некоторого временного промежутка. Если ключевые показатели пришли в норму, виден позитивный тренд, то отрасль или организация может быть снята с контроля.

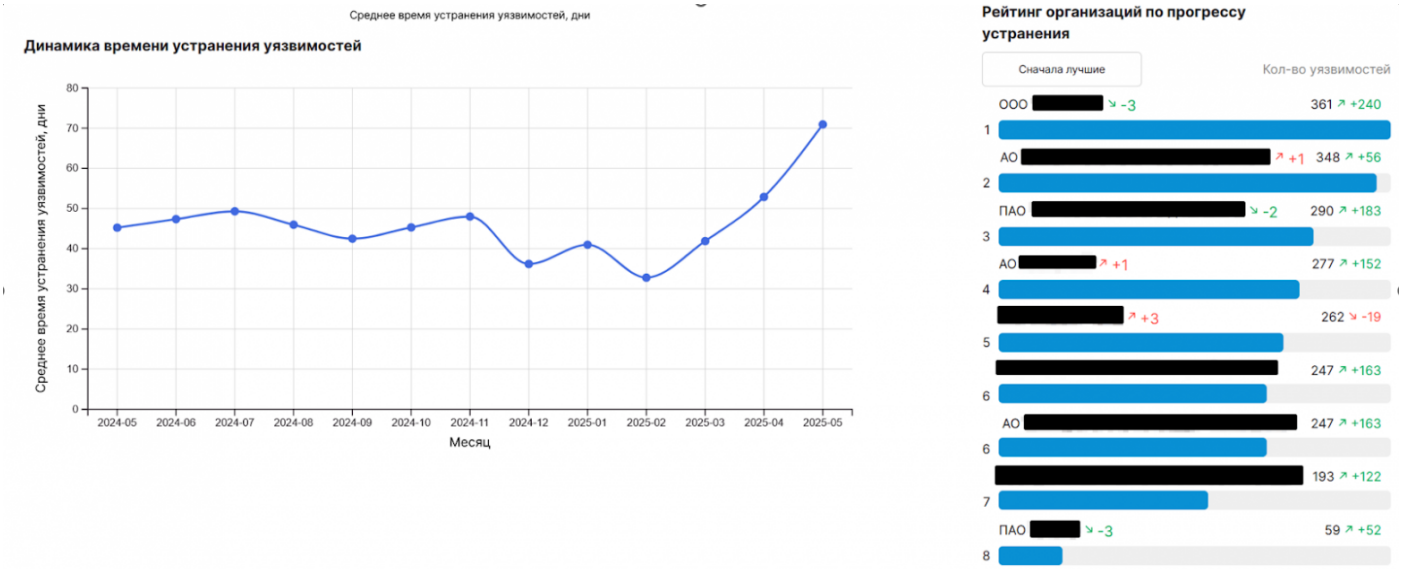
Все последующие блоки либо помогают лучше понять проблемы региона в целом, либо провести сравнительный анализ организаций по другим характеристикам. Также помимо метрик, мы поработали над обоснованием негативной или позитивной обратной связи, как с точки зрения законодательства, так и с точки зрения лучших практик в сфере информационной безопасности.

Группы ресурсов, нерекомендуемых к публикации

Так, к примеру, на рисунке X изображены:

- группы ресурсов, нерекомендуемых к публикации;
- изменение их количества от месяца к месяцу;
- какие нормативные акты нарушаются фактом их присутствия на внешнем периметре.

Примером более детальной характеристики, которая может показать положения дел региона в целом и наиболее отличившихся в положительную сторону, может быть время устранения уязвимости.



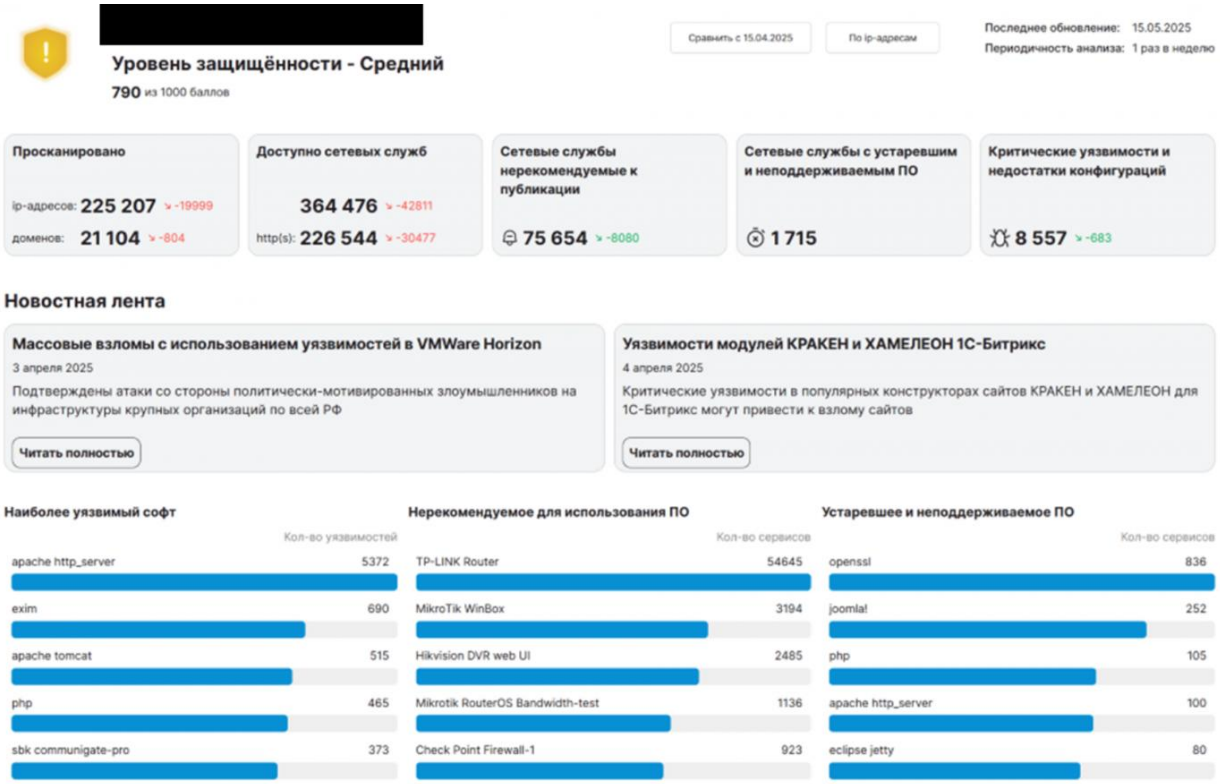
Рейтинг организаций по прогрессу устранения уязвимостей

Представьте себе большую организацию, у которой тысячи ресурсов на внешнем периметре, она серьезно занимается ИБ, но при этом уязвимости не перестают появляться. Ввиду количества информационных систем и их разнообразия, недостатков будет много, как следствие, уровень защищенности в моменте может быть низким. Но поскольку организация эффективно занимается их устранением – риски сильно снижаются. И по задумке грамотный ответственный посмотрит не только на ситуацию в моменте, но и на то, как организация реагирует на возникающие перед ней вызовы.

Кроме того, график с динамикой устранения уязвимостей на большом промежутке времени может подсветить нарастающую проблему раньше, чем она пройдет точку невозврата.

Взгляд со стороны. А что делать технарям?

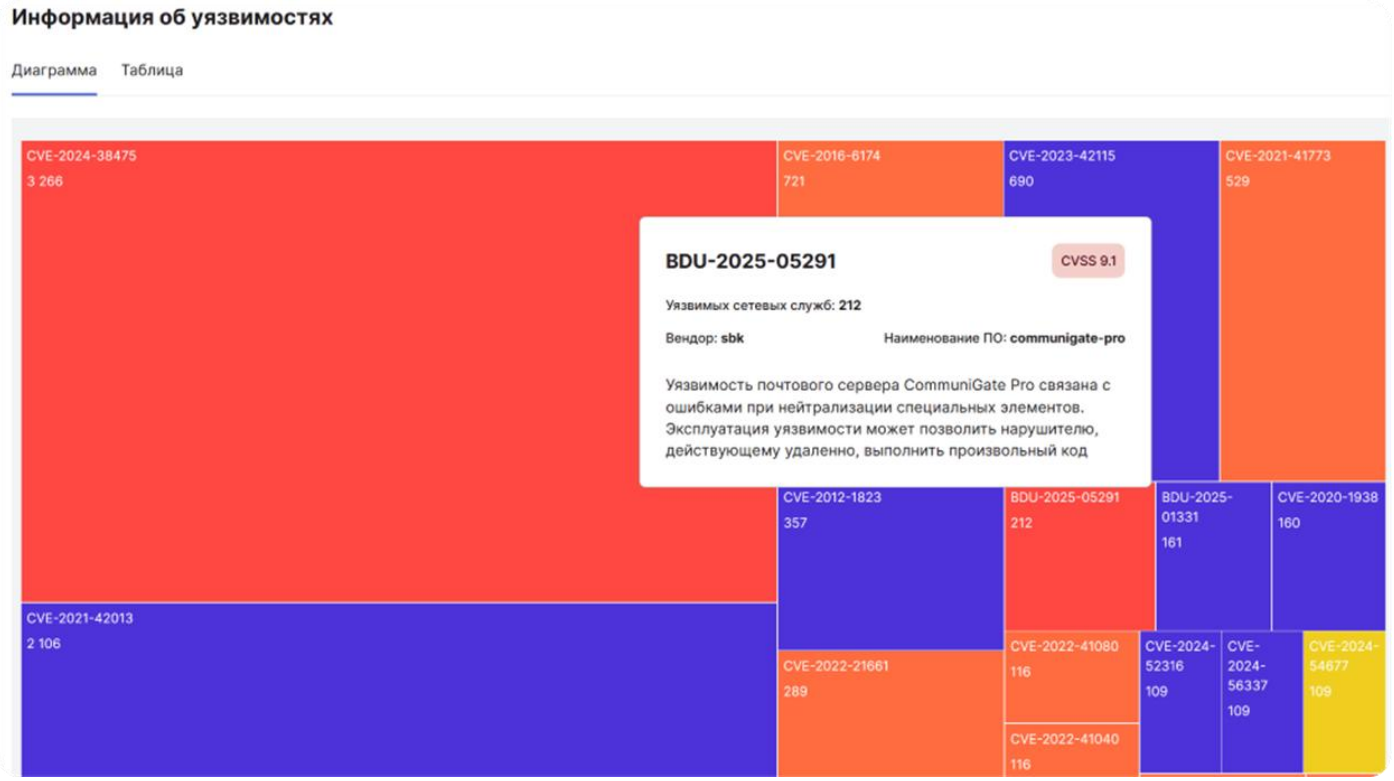
Про исключительно организационный уровень мы поговорили, давайте теперь попробуем представить себя на месте человека, который отвечает технически за безопасность целого региона.



Интерфейс уровня региона с детализацией по информационным ресурсам

Для такого пользователя интерфейс выглядит похожим образом, но отличается по наполнению:

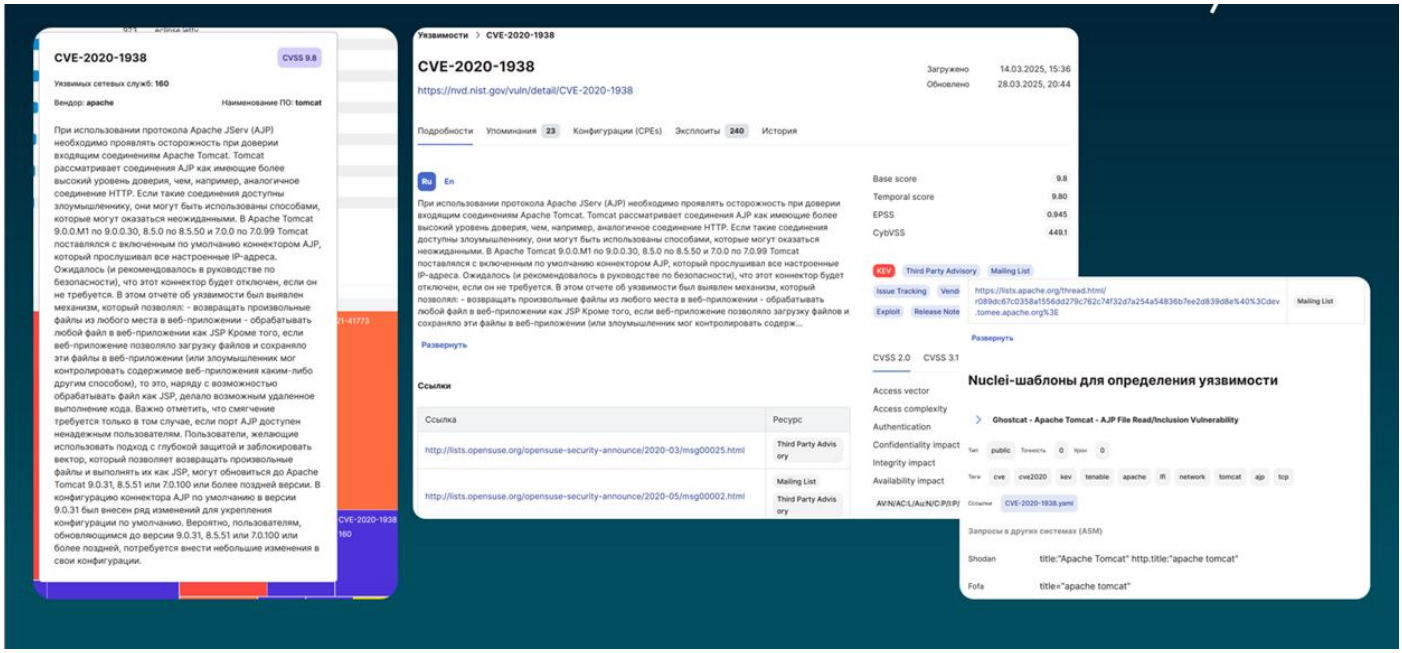
1. Приборная панель, на которой отражены ширина поверхности потенциальной атаки и оценки по разным классам недостатков сервисов.
2. Новостная лента, на которую пользователь смотрит уже с более технической стороны и может предположить риск возможной эпидемии.
3. Рейтинги типов ПО, на которые стоит обратить внимание. К примеру, в качестве поручения по организациям могут быть разосланы методические материалы по обновлению определенного программного обеспечения. Предполагается, что если сконцентрироваться на наиболее распространенном и уязвимом, а не отправлять огромный список, то подконтрольные организации с бОльшей вероятностью примут рекомендации ко вниманию и минимизируют угрозу не только для себя, но и для целого региона.



Интерфейс с информацией об уязвимостях

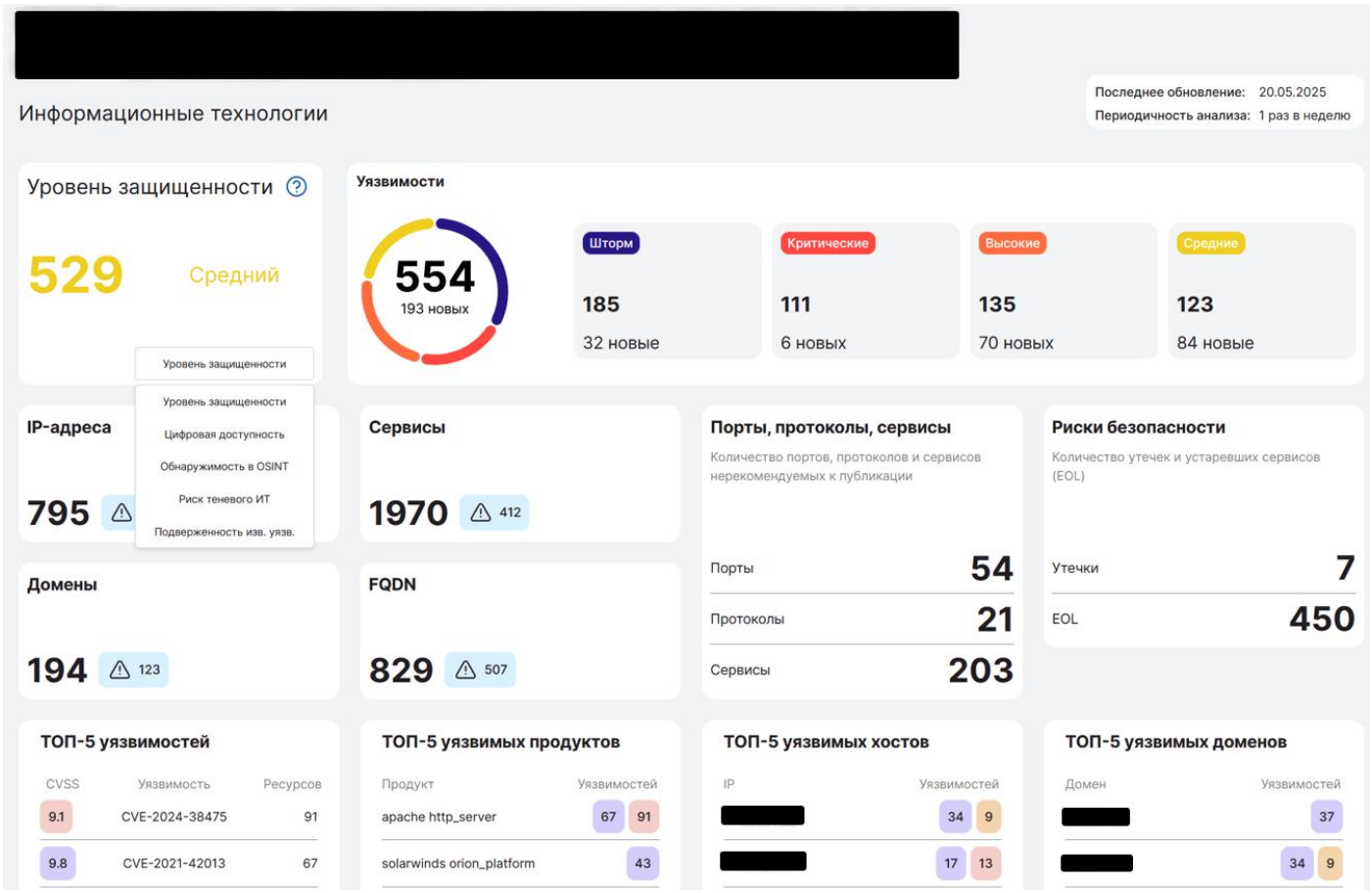
Аналогично программному обеспечению, внимание можно обратить и на наиболее критичные и распространенные уязвимости. В данном блоке можно оценить количество ресурсов (площадь прямоугольника), которые были затронуты той или иной уязвимостью, ее критичность (по цвету) и получить краткую информацию при наведении.

Дополнительные данные берутся из базы знаний об уязвимостях под названием Vulnum – на текущий момент внутренней разработки, агрегирующей описание недостатков, связанные источники, эксплойты, nuclei-шаблоны и другую полезную информацию. Пример подробностей об уязвимости с идентификатором CVE-2020-1938 представлен на рисунке ниже.



Интерфейс Vulnum с подробной информацией об уязвимостях

Последний дашборд, который хотелось бы представить, является последним этапом декомпозиции. Он может быть полезен, как для человека, технически отвечающего за информационную безопасность региона, который решил получить фактуру по конкретной организации, так и для владельца информационных систем данной организации. Помимо уже перечисленных метрик и показателей добавляется несколько, которые позволяют получить исчерпывающую информацию как о поверхности атак, так и о том, как выглядит периметр извне для потенциального злоумышленника. К примеру, возможность получения информации о периметре организации из публичных источников (GASM).



Интерфейс уровня организации

Также стоит отметить блок с рисками безопасности – это те недостатки, которые на текущий момент не предоставляют опасности, но в произвольный момент времени могут превратиться в угрозу – выход новой уязвимости, которую будут исправлять с низкой вероятностью (из-за прекращения поддержки продукта), или утечка с парой учетных данных, которая может подойти к сервису, планируемого к публикации на внешнем периметре.

Специалист, работающий с данным дашбордом, может получить информацию вплоть до конкретных ресурсов.

Но в случае использования любых метрик возникает вопрос – насколько они отражают действительность? Давайте попробуем погрузиться в то, из чего они складываются и как собирается эта информация.

Откуда данные?

Напомню, что начали мы с конца, а вот теперь перейдем к началу :) Для нашей компании данный проект был не только вызовом, но и кладезем интересных технических задач:

1. Что из себя представляет регион?
2. Как из 8000 уязвимостей выбрать важные?
3. Доступная камера – просто мисконфигурация или непросто?

Список вопросов выше – это маленькая часть, которой мы хотели бы поделиться и которая отражает этапы формирования индекса.

Итак, что из себя представляет регион? Мы сами до конца не знаем, но, чтобы максимально приблизиться к действительности, нами были использованы 2 основных подхода: от ресурсов и от организации.

В подходе от ресурсов были использованы базы соответствия географического расположение и IP-адресов, а также собственный whois.

С точки зрения правительства, контролируемые информационные системы – это все-таки часть организации, и далеко не всегда они хостятся в данном регионе (не будем забывать про многообразие хостеров, облака, распределение по нескольким ЦОД-ам для безотказности и так далее).

Мы с коллегами из Innostage составили список из 150 критических организаций, в который впоследствии сократился до 80.

Далее при помощи разработанной СайберОК технологии NetSlicer был осуществлен сбор ресурсов. Данный продукт использует итеративный подход с применением ML-модели, каждый следующий цикл которого приносит некоторое количество доменных имен и IP-адресов, относящихся к организации из разных источников, включая СКИПА. Затем происходит этап фильтрации данных, после которого шаги повторяются. Поиск останавливается после того, как очередная итерация перестает приносить дополнительную информацию.

Объединяя эти 2 подхода, были получены порядка 680 000 IP-адресов и 30 000 доменных имен.

Сканирование

Следующий шаг после сбора целей – сканирование. В нашем случае – сканирование на уязвимости (всё строго с согласованием и кучей бумажек). Нами были использованы 3 подхода разной степени агрессивности в зависимости от ресурсов:

1. Использование исторических данных (подходит только при первой итерации).

2. Механизм cpe2cve с фильтрацией уязвимостей на основании внутренней базы знаний СайберОК об уязвимостях Vulnum.

- AV:N.
- CVSS > 7.0.
- Наличие эксплойта.
- Ограничение по списку cpe.

3. Активное сканирование для ограниченного списка организаций (весь арсенал проверок).

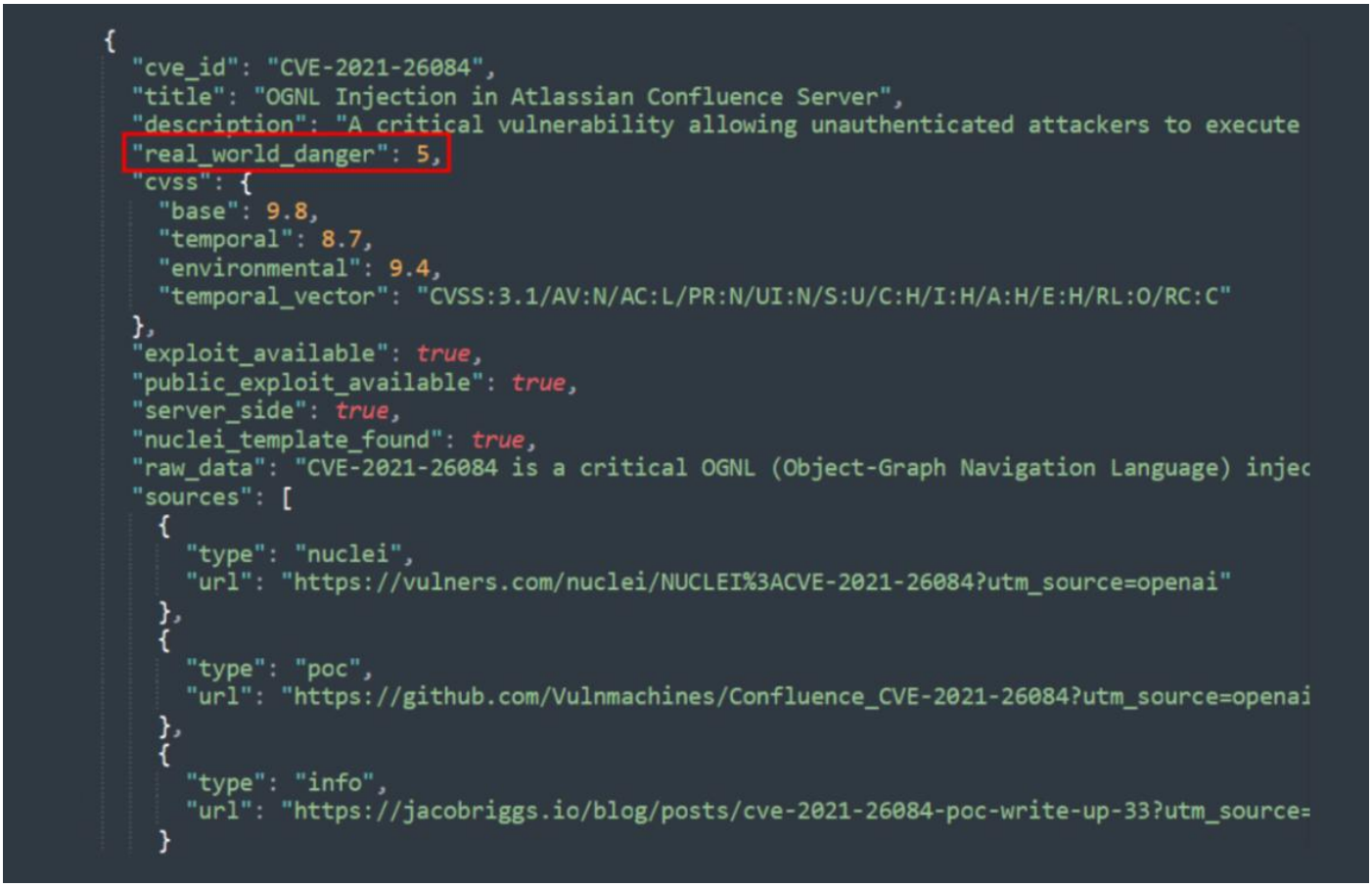
Самым интересным для нас был второй подход, потому что решалась довольно известная всем проблема – как из портянки множества баннерных уязвимостей (определенных по версии) выявить те, которые действительно могут нести угрозу и с бОльшей вероятностью будут использованы злоумышленниками в дикой среде.

Нами был использован следующий подход. Во-первых, были отфильтрованы некоторые cpe, в которых применение патча не связано с изменением версии. Далее были отфильтрованы только те уязвимости, которые в базе Vulnum-а содержат хотя бы один эксплойт, имеют метрику CVSS больше 7 и сетевой вектор атаки. При помощи такой фильтрации количество уникальных идентификаторов удалось сократить с ~ 8100 до 335. Данный подход имеет понятные недостатки, связанные, например, с потерей некоторого количества уязвимостей, имеющих локальный вектор, но использующихся в цепочках (Exchange). Также стоит отметить, что мы никак не учитываем сложность потенциальной эксплуатации.

Следующий подход, который был применен, это использование технологии на базе LLM под кодовым названием Onotolle (ну вот потому что). На вход подается некоторая информация об уязвимости, на выходе получаем метрику real_world_danger, которая говорит об опасности данного недостатка. Минимальные данные, которые необходимо передать, это идентификатор и cpe. В нашем случае мы использовали всю информацию по уязвимости, которая была собрана Vulnum-ом, с границей 4 метрики real_world_danger.

В результате из тех же ~ 8100 уязвимостей было выбрано ~ 211 важных, из которых 178 имели real_world_danger равный 4 и 33 равный 5 соответственно. При ручном анализе получившихся данных лишь по 10% недостатков оценка эксперта и технологии Onotolle не совпала.

```
CVE-2007-0494,isc,bind
CVE-2021-26084,atlassian,confluence_server
CVE-2022-26134,atlassian,confluence_server
```



Пример входящей и исходящей информации технологии Onotolle

Страшилка про публично доступные камеры

Как показывает практика, помимо стандартных уязвимостей и мисконфигураций сетевых сервисов, на информационную безопасность организации – и тем более региона – влияют и более нестандартные сущности. В качестве примера можно привести публично доступные камеры.

Совсем страшное не будем рассказывать, поделимся умеренно-страшным:

1. Объемы в масштабах Рунета – десятки тысяч и тысячи на масштабах региона.
2. При помощи VLM данная информация становится источником получения видео по ключевым словам или даже запросу.
3. К сожалению, в собираемых подобным способом данных, помимо ТЦ, кафе, wildbirries-ов, лифтов, парковок есть и объекты государственной важности.

Данный пример еще раз напоминает о том, что задача информационной безопасности на масштабах региона требует комплексного подхода и как можно большего количества различных сущностей, которые могут быть собраны на внешнем периметре. Кто знает, какая деталь будет использована в следующей атаке.

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Итоги

На текущий момент:

1. Нами была проведена первая итерация, включающая в себя несколько сканирований и сбор информации.
2. Была сформирована первая версия индекса киберустойчивости и сопутствующих метрик.
3. Были переданы данные регуляторам и организациям.
4. На ряде критичных организаций были подключены пентестеры из PentOps – нашего сервиса непрерывного тестирования на проникновение внешнего периметра.
5. В результате этого были обнаружены множество уязвимостей, включая трендовые и эксплуатируемые в дикой природе.
6. А сейчас мы с нетерпением ждем следующих серий!

Теперь перед нами стоит задача помощи в устранении, следующих итераций и постоянного контроля, поскольку периметр дышит и не стоит на месте.

Пусть за каждой метрикой будет действие!